目次

第 1 章　安全ライフサイクルにおけるハードウエアエンジニアリング 6

1.1　ハードウエアエンジニアリングの役割 7

1.1.1　ハードウエアエンジニアリングの目的 7

1.1.2　ハードウエアエンジニアリングの活動 8

1.2　安全ライフサイクルにおけるハードウエアエンジニアリング 9

1.2.1　ハードウエアエンジニアリングにおける安全活動 9

第 2 章　ハードウエア安全要求の仕様化 10

2.1　ハードウエア安全要求の仕様化の概要 11

2.1.1　ハードウエア安全要求仕様化の目的 11

2.1.2　ハードウエア安全要求仕様化の活動 11

2.2　ハードウエア安全要求仕様化の詳細解説 12

2.2.1　ハードウエア安全要求の定義 12

2.2.2　ハードウエアとソフトウエア間のインタフェース仕様（HSI）の更新 16

2.2.3　ハードウエア安全要求の検証 16

2.2.4　ハードウエアとソフトウエア間のインタフェース仕様（HSI）の検証 16

セルフチェックリスト：ハードウエア安全要求の仕様化 17

第 3 章　ハードウエア設計 18

3.1　ハードウエア設計 19

3.1.1　ハードウエア設計の目的 19

3.1.2　ハードウエア設計の活動 19

3.2　ハードウエア設計の詳細解説 21

3.2.1　ハードウエアアーキテクチャ設計 21

3.2.2　ハードウエア詳細設計 22

3.2.3　ハードウエア設計の検証 23

セルフチェックリスト：ハードウエア設計 26

第 4 章　ハードウエアアーキテクチャ設計の評価 28

4.1　ハードウエアアーキテクチャメトリック評価の概要 29

4.1.1　ハードウエアアーキテクチャメトリック評価の目的 29

4.1.2　ハードウエアアーキテクチャメトリック評価の活動 29

4.2 ハードウエアアーキテクチャメトリック評価の詳細解説 30
4.2.1 フォールトと故障 30
4.2.2 シングルポイントフォールトメトリック（SPFM）の計算 31
4.2.3 潜在フォールトメトリック（LFM）の計算 33
4.2.4 ハードウエアアーキテクチャメトリックの評価手順 34
4.2.5 ハードウエアアーキテクチャメトリック評価結果の検証レビュー 39
セルフチェックリスト：ハードウエアアーキテクチャ設計の評価 40

第 5 章 ランダムハードウエア故障による安全目標侵害の評価 42

5.1 ランダムハードウエア故障による安全目標侵害評価の概要 43
5.1.1 ランダムハードウエア故障による安全目標侵害評価の目的 43
5.1.2 ランダムハードウエア故障による安全目標侵害評価の活動 43
5.2 ランダムハードウエア故障による安全目標侵害評価の詳細解説 44
5.2.1 評価手法の選択 44
5.2.2 安全目標侵害確率の評価（PMHF） 44
5.2.3 安全目標侵害の各原因の評価（EEC） 48
5.2.4 検証レビューの実施 50
セルフチェックリスト：ランダムハードウエア故障による安全目標侵害の評価 51

第 6 章 ハードウエア統合と統合テスト 52

6.1 ハードウエア統合と統合テストの概要 53
6.1.1 ハードウエア統合と統合テストの目的 53
6.1.2 ハードウエア統合と統合テストの活動 53
6.2 ハードウエア統合と統合テストの詳細解説 54
6.2.1 ハードウエア統合テストの計画 54
6.2.2 ハードウエア統合テストの設計 54
6.2.3 ハードウエア統合及び統合テストの実施 59
セルフチェックリスト：ハードウエア統合と統合テスト 60

第 7 章 【共通エンジニアリング】安全要求管理 62

7.1 安全要求定義 63
7.1.1 安全要求定義の目的 63
7.1.2 安全要求記述に対する要求事項 63
7.2 安全要求の管理 66
7.2.1 安全要求管理の目的 66
7.2.2 安全要求管理への要求事項 66

第 8 章　【共通エンジニアリング】安全分析 68
8.1　安全分析 69
8.1.1　安全分析の目的 69
8.1.2　安全分析の技法 70
8.2　従属故障分析 76
8.2.1　従属故障分析の目的 76
8.2.2　従属故障分析の手順 76
8.2.3　カップリングファクタ識別の考慮点 79
第 9 章　【共通エンジニアリング】ASIL 依存のエンジニアリング 82
9.1　ASIL デコンポジション 83
9.1.1　ASIL デコンポジションの目的 83
9.1.2　ASIL デコンポジション適用における考慮点 84
9.2　異なる ASIL エレメントの共存 85
9.2.1　異なる ASIL エレメントの共存　活動の目的 85
9.2.2　異なる ASIL エレメントを共存させるための考慮点 86
第 10 章　【共通エンジニアリング】既存エレメントの利用 88
10.1　既存エレメントの再利用 89
10.1.1　既存エレメント再利用の目的 89
10.1.2　既存エレメント開発における役割 89
10.2　影響分析 90
10.3　安全関連系への COTS 利用 91
10.3.1　ソフトウエア COTS の利用 91
10.3.2　ハードウエア COTS の利用 92
10.4　安全関連系への SEooC 利用 93
10.4.1　SEooC 開発の流れ 93
10.4.2　想定の開発と利用の評価 94
10.4.3　SEooC の統合と評価 94